

# ANALYSIS OF ORIGINAL BILL

## Franchise Tax Board

Author: Bowen Analyst: Darrine Distefano Bill Number: SB 147  
Related Bills: See Legislative History Telephone: 845-6458 Introduced Date: January 30, 2001  
Attorney: Patrick Kusiak Sponsor: \_\_\_\_\_

**SUBJECT:** Prohibit Employers From Secretly Monitoring Employee Electronic Mail Or Computer Records

### SUMMARY

This bill would prohibit employers from monitoring their employees' electronic mail or other computer-generated records without informing them.

### PURPOSE OF THE BILL

According to the author's staff, the purpose of this bill is to require that private and public employers notify their employees that all electronic data generated by the employee will be monitored.

### EFFECTIVE/OPERATIVE DATE

This bill would be effective January 1, 2002, and operative after that date.

### POSITION

Pending.

### ANALYSIS

#### STATE LAW

Existing state law prohibits a state officer or employee from engaging in any employment, activity, or enterprise that is clearly inconsistent, incompatible, in conflict with, or inimical to his or her duties as a state officer or employee. State law also requires state agencies to adopt rules governing the application of these laws and to notify state officers and employees of the existence of these laws and their application to the employee upon the employee's employment.

Due to the nature of the confidential services provided by the Franchise Tax Board (FTB), the department has established a policy regarding the use of email and the Internet. FTB employees are prohibited from using email and the Internet for any unauthorized disclosure of confidential or proprietary information; for any private or personal business gain; for any illegal purpose; or for transmitting threatening, obscene, or harassing messages. Employees are notified that all electronic mail is the property of FTB. Management can access and review the contents of an employee's email to ensure compliance with the policy. Management also has the right to disclose email messages to law enforcement during the course of an investigation.

#### Board Position:

_____ S	_____ NA	_____ NP
_____ SA	_____ O	_____ NAR
_____ N	_____ OUA	_____ X PENDING

#### Department Director

#### Date

Gerald H. Goldberg

4/20/01

This policy is posted on FTB's internal intranet website and a hard copy is distributed to all permanent employees on an annual basis. All new and seasonal employees are also given a copy of the policy to review and sign upon commencement of their employment.

### THIS BILL

This bill would prohibit an employer from secretly monitoring an employee's electronic mail or any computer-generated records. This bill would define "secretly monitor" to mean inspect, review, or retain electronic mail or other computer records in a manner that does not comply with the policies and practices that are disclosed to the employee.

This bill would require an employer that intends to inspect, review, or retain any electronic mail or any other computer records to notify its employees of its workplace privacy and electronic monitoring policies and practices. New employees will be notified at the start of their employment and, for existing employees, notification will be no later than March 1, 2002. The employer may provide notification by presenting the policies and practices in hard copy or by electronic mail.

An employer will be in compliance with this notification requirement if it: (1) includes the notice in the employee handbook or electronically posts the notice on the employee's computer screen; and (2) receives electronic verification that the employee has received, read, and understood the notice.

This bill also would require employees to sign a statement acknowledging that he or she has read, understood, and acknowledged receipt of the employer's electronic monitoring policies and practices.

If an employee refuses to sign or electronically verify the employer's electronic monitoring policies and practices, the person who provided the employee with the policies and practices will sign and retain a statement to that effect. The employer will be in compliance with this bill when a copy of the signed statement has been given to the affected employee.

This bill would define "employee" to include an individual employed by the state or any organizational subdivision; any county, city, or city and county; any school district, community college district, or the University of California; or any political subdivision or public corporation of the state.

### IMPLEMENTATION CONSIDERATIONS

As stated above under State Law, FTB has a policy regarding the use of email and the Internet that is communicated to all employees on an annual basis. Employees are notified that all electronic mail and computer records are property of FTB and will be monitored by management for compliance with that policy. Consequently, implementation of this bill would not significantly impact the department.

### **LEGISLATIVE HISTORY**

SB 1016 (Bowen 1999/2000) and SB 1822 (Bowen 1999/2000), would have prohibited an employer from secretly monitoring the electronic mail or other computer records generated by an employee. Both bills were vetoed by the Governor for placement of undue regulatory burdens and potential legal exposure on businesses.

## **PROGRAM BACKGROUND**

Over the past 15 years, businesses and individuals have become increasingly dependent upon email and various other computer programs to communicate. In order to deal with the privacy issues that accompany the use of electronic communications, businesses and individuals have turned to federal and state government for guidelines on the appropriate levels of monitoring and the protection of personal electronic privacy.

In 1986, Congress revamped the Electronic Communications Privacy Act (ECPA), addressing the legal privacy issues that evolved from the growing use of computers and other new innovations in electronic communications. The ECPA updated Title III of the Omnibus Crime Control and Safe Streets Act of 1968 that had been designed to clarify what constitutes invasion of privacy when electronic surveillance is involved. The ECPA extended privacy protection to apply to radio paging devices, electronic mail, cellular telephones, private communication carriers, and computer transmissions.

The ECPA was designed to protect the contents of stored electronic mail, voice mail, and remote computing services. It also was intended to prohibit providers of electronic communication services from disclosing the contents of communication that has been stored electronically without the lawful consent of the person who originated the communication. However, the ECPA does allow employer eavesdropping if employees are notified in advance or if the employer has reason to believe the company's interests are in jeopardy.

## **OTHER STATES' INFORMATION**

Research of other states did not disclose any statutes that expressly permit an employer to monitor an employee's electronic mail or computer records.

## **FISCAL IMPACT**

This bill would not significantly impact the department's costs.

## **ECONOMIC IMPACT**

This bill would not impact the state's income tax revenues.

## **LEGISLATIVE STAFF CONTACT**

Darrine Distefano  
Franchise Tax Board  
845-6458

Brian Putler  
Franchise Tax Board  
845-6333